UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/841,950	04/08/1997	MARK D. RIGGINS	40827.00004	3712

7590 11/17/2006		EXAMINER
Jinntung Su		TRUONG, THANHNGA B
MANATT, PHELPS LLP		
1001 Page Mill Road	ART UNIT	PAPER NUMBER
Building 2	2135	
Palo Alto, CA 94203		

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	08/841,950	RIGGINS, MARK D.
	Examiner	Art Unit
	Thanhnga B. Truong	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>10 October 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>2-6, 8-14, 16-20 and 22-29</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>2-6, 8-14, 16-20 and 22-29</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

AU 2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date <u>10/10/06</u>.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to the communication filed on October 10, 2006.
Claims 2-6, 8-14, 16-20, and 22-29 are pending.

Continued Examination Under 37 CFR 1.114

2.   A request for continued examination under 37 CFR 1.114, including the
fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an
Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935).
Since this application is eligible for continued examination under 37 CFR 1.114, and the
fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has
been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on October 10,
2006 has been entered. However, an in-depth reviewed and a thorough search by the
examiner, a new ground(s) of rejection is addressed herein. At this time, claims 2-6, 8-
14, 16-20, and 22-29 are rejected.

Information Disclosure Statement

3.   The information disclosure statement (IDS) submitted on October 10,
2006 was filed after the mailing date of the notice of allowance on May 10, 2006. The
submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the
information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for
all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 2-6, 8-14, 16-20, and 22-29 rejected under 35 U.S.C. 103(a) as
being unpatentable over He et al (US 6,088,451), and further in view of Komatsu et al
(US 4,817,050).

        a.   *Referring to claim 6:*

           i.   He teaches a system on a server computer system (see Figures 2 and 10 of He), comprising:

           (1)   a communications engine for establishing a communications link with a client **(column 4, lines 4-7 of He);**

           (2)   security services (e.g., authentication server) coupled to the communications engine for presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option according to at least one user authentication protocol and for determining user privileges based on the identity of the user and the level of authentication **(see Figure 2 and more details on column 7, lines 55-67 through column 9, lines 1-24 of He);**

           (3)   a web server (e.g., one of the network elements) for presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted, and for enabling the client to select a particular service from the set of available services **(column 6, lines 20-67 through column 7, lines 1-2 of He);**

           (4)   a host engine (e.g., one of the network elements) coupled to the security services and to the web server for providing to the client service communication code that enables communication with the particular service **(see Figure 2 and more details on column 11, lines 53-67 through column 12, lines 1-64 of He); and**

           (5)   a keysafe (e.g., database) for storing keys (e.g., unique user identifier), each key for enabling communication between the client and a respective service from the set of available services and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them **(column 12, lines 53-55; column 16, lines 27-67 through column 17, lines 1-27 of He).**

ii.   Although He teaches all user account information will then be stored in a database and managed exclusively at the site of the authentication server 202, wherein a registration database (Reg. DB) 210, however, can also be accessed by the credential server 204 and the network element access server 206, in addition to the authentication server 202; and generally, the user account record is created in the registration database 210 at the same time as the generation of the unique user identifier, He is silent on the capability of directly disclosing that the database could be storing keys (if indeed is not inherently in He's system). On the other hands, Komatsu teaches:

(1)   database system for storing key data as in **column 2, lines 28-34 of Komatsu.**

iii.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1)   have modified the invention of He with the teaching of Komatsu (if indeed is not inherently in He's system) for storing medical data including image data such as diagnostic images **(column 1, lines 7-9 of Komatsu).**

iv.   The ordinary skilled person would have been motivated to:

(1)   have modified the invention of He with the teaching of Komatsu to provide a database system whose processing efficiency is improved **(column 2, lines 15-17 of Komatsu).**

b.   _Referring to claims 2, 16:_

i.   He further teaches :

(1)   wherein the communications engine uses SSL to create a secure communications link with the client **(column 4, lines 54-67 through column 5, lines 1-3 of He).**

c.   _Referring to claims 3, 17:_

i.   He further teaches :

(1)   wherein the communications engine negotiates an encryption protocol for transferring messages to and from the client **(column 2, lines 66-67 through column 3, lines 1-15 of He).**

       d.   *Referring to claims 4, 18:*

          i.   He further teaches :

          (1)   wherein the communications engine uses public key certificates for transferring messages to and from the client **(column 13, lines 52-63 of He).**

       e.   *Referring to claims 5, 19:*

          i.   He further teaches :

          (1)   wherein the security services uses public key certificates to authenticate a user of the client to determine the user privileges **(column 13, lines 52-63 of He).**

       f.   *Referring to claim 8:*

          i.   He further teaches :

          (1)   wherein the security services use a digital signature (e.g., certificate or ticket) to authenticate the user to determine the user privileges **(column 13, lines 52-63 of He).**

       g.   *Referring to claim 9:*

          i.   He further teaches :

          (1)   wherein the host engine forwards to the client security code for enabling the client to perform a security protocol recognized by the security services **(column 12, lines 65-67 through column 13, lines 1-42 of He).**

       h.   *Referring to claim 10:*

          i.   He further teaches :

          (1)   wherein one of the available services is secured by a firewall (e.g., router) and one of the keys includes the additional authentication information to enable communication through the firewall **(column 4, lines 1-27 of He).**

       i.   *Referring to claim 11:*

          i.   He further teaches :

          (1)   a firewall (e.g., router) for protecting the system **(column 4, lines 1-27 of He).**

       j.   *Referring to claim 12:*

        i.   He further teaches :

        (1)   wherein one of the keys includes an address identifying the location of the selected service **(column 13, lines 35-42 of He).**

    k.   *Referring to claim 13:*

        i.   He further teaches :

        (1)   wherein the code uses a key to provide to the client a direct connection with the selected service **(column 13, lines 35-42 of He).**

    l.   *Referring to claim 14:*

        i.   He further teaches :

        (1)   a proxy (e.g., authentication server) for communicating with the selected service **(column 11, lines 53-67 through column 12, lines 1-64 of He)**, and wherein the code enable the client to communicate with the proxy and one of the keys enables the proxy to locate the selected service **(column 13, lines 35-63 of He).**

    m.   *Referring to claims 20 and 29:*

        i.   These claims have limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

    n.   *Referring to claims 22-28:*

        i.   These claims have limitations that is similar to those of claims 8-14 respectively, thus they are rejected with the same rationale applied against claims 8-14 respectively above.

    6.   Claims *10, 11, 14, 24, 25, and 28* rejected under 35 U.S.C. 103(a) as being unpatentable over He et al (US 6,088,451), in view of Komatsu et al (US 4,817,050), and further in view of Boyle et al (US 5,872,847).

    a.   *Referring to claims 2, 10, 11, 14, 16, 24, 25, and 28:*

        i.   The combination of teaching between He and Komatsu teaches a system on a server computer system as shown in Figures 2 and 10 of He. Even though He uses router, which is one of the firewalls, as described in **column 4, lines 1-27** and protocol for SSL handshaking between the computer network, as describe in **column 4, lines 54-67 through column 5, lines 1-3,** He and Komatsu are

silent on the capability of technically using firewall or guard and proxy for communicating with selected service. On the other hand, Boyle teaches as shown in Figure 1 and for further details of an MLS network system using trusted associations to establish trust in a computer network (column 5, lines 30-61; and column 12, lines 30-57 of Boyle).

      ii.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

      (1)   have modified the modified-invention of He with the teaching of Boyle (if indeed is not inherently in He's system) to establishing trust between secured users in a computer network environment **(column 1, lines 16-17 of Boyle).**

      iii.   The ordinary skilled person would have been motivated to:

      (1)   have modified the modified-invention of He with the teaching of Boyle to provide a security method capable of discovering needed trusted information over a computer network when that information is needed without any requirement for global configuration data **(column 3, lines 25-28 of Boyle).**

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Chander B. Thy
AU2135

TBT

November 13, 2006